REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-13 and 15-20 are pending. Claims 14 and 21-22 are canceled by this reply, without prejudice or disclaimer. Claims 1 and 15 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 15.

Claim Amendments

Independent claims 1 and 15 are amended to clarify aspects of the invention. Corresponding dependent claims are amended for purposes of consistency and to correct minor informalities. No new matter is added by way of these amendments, as support is found at least in the originally filed claims and in paragraph [0053] of the publication of the present application (US Pub. No. 2007/0253551).

Rejection(s) under 35 U.S.C. § 112

Claims 16 and 22 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Specifically, the Examiner asserts that the means-plus-function language in claims 16 and 22 renders the claims indefinite as one possible means described in the specification is software. Claim 22 is canceled by this reply; thus, this rejection is moot for claim 22. Claims 16 is amended to remove the means plus function language, and to recite a hardware element, a receiver, for receiving the broadcast encrypted control data. Accordingly, the claims are now definite. Withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C. § 102

Claims 1-7, 11-16, and 19-22 are rejected under 35 U.S.C. § 102(e) as being anticipated by US Pub. No. 2006/0107045 ("Buhan"). Claims 14 and 21-22 are canceled by this reply; thus, this rejection is now moot with respect to the canceled claims. To the extent that this rejection may still apply to the remaining amended claims, this rejection is respectfully traversed.

The claimed invention is related to pairing a decoder and a portable security module, the decoder and the portable security module being adapted to descramble scrambled audiovisual information received by the broadcast network. The broadcasting center sends the same message to all decoding systems; it is therefore not possible to have such a message encrypted by a key pertaining to one decoding system, one decoder, or one security module. Thus, the solution proposed by the present invention is to randomly select a first key k1 and to assign it to the decoder and to calculate a second key k2 based on the first key and assign it to a portable security module, thereby pairing the decoder and portable security module together, so that the combination of the first and the second key is the same for all receiving units.

Accordingly, the independent claims require, in part, (i) a first key and a second key *according to* the first key; (ii) wherein *a combination* of the first and second key enables decryption of common (*i.e.*, across a plurality of receiving decoding systems) received encrypted data; and (iii) assigning the first key to a decoder and the second key to a portable security module to pair the decoder with the portable security module. That is, some combination of two distinct keys, one made according to the other, results in a pairing key that can be used across a plurality of receiving decoding systems, each having a decoder/portable security module pair, to

decrypt data. The pairing key is formed between a pair of one decoder and one portable security module with which the first and second keys are respectively associated.

Turning to the rejection, "[a] claim is anticipated only if *each and every element* as set forth in the claims is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987) (emphasis added). Further, "[t]he identical invention must be shown in as complete detail as is contained in the claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). Applicants assert that Buhan fails to disclose each and every element of the independent claims.

In contrast to the claimed invention, Buhan merely provides a method of setting up a secure channel between a terminal module (CT) and a converter module (CC), which is described in detail in paragraphs [0048]-[0050] of Buhan. It appears that the Examiner equates the claimed first key with Buhan's public key PK and the claimed second key with the corresponding private key of the asymmetric key pair disclosed in Buhan. *See* Action, page 3. However, Buhan is completely silent with respect to the public and private keys of the pair of asymmetric keys being combined in any way to form a pairing key. Rather, each of the public and private keys is used, *separately*: the public key by the terminal module to encrypt a session key, and the private one by the converter module to decrypt the session key (*see* Buhan, paragraph [0048] – [0049]). In other words, while the public and private keys correspond to one another for the asymmetric encryption algorithm to operate, there is no *combination* of the public and private key contemplated in Buhan.

"[U]nless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed, and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN, Inc. v. VeriSign, Inc.*, 2008 WL 4614511 (Fed. Cir. 2008). Thus, in view of *Net MoneyIN*, Buhan fails to disclose (ii) as required above.

Further, with respect to (ii), the focus of the asymmetric encryption algorithm is not the decryption of encrypted scrambled broadcast network data, but rather, is directed only to secure communication between the terminal module and the converter module. In fact, the decryption in Buhan works just as well using a non-encrypted channel between the devices. As such, there is no explicit disclosure in Buhan that a combination of the public key and the session key is what allows for decryption of data in Buhan, as also required by (ii) above. In contrast, Buhan explicitly discloses in paragraph [0046] that "terminal modules (CT)...allow the decryption of the network data at the level of the device (TV1, TV2, PC) thanks to the network key (NK) stored in each module." Buhan is thus quite clear that it is the network key that allows decryption of the data, and the network key is also NOT a combination of the public key and the private key of the asymmetric algorithm. Accordingly, no combination of keys in Buhan allows for decryption of digital content, as required by the claimed invention.

The way Buhan uses the predetermined 'first key' and the randomly generated 'second key' does not, in any way, result in assigning the first key to one component of a pair in Buhan and the second key to the other component in the pairing. In Buhan, the 'pairing' is the establishment of the secure communication, which occurs between two devices (CT and CC) that *already* have the necessary public/private key pairs. The only thing that is passed between

the devices is the session key SK. Accordingly, there is no assignment of the public key to the CT and the private key to the CC in Buhan, as required by (iii) above.

In view of the above, the Examiner's contentions fail to support an anticipation rejection of the amended independent claims. Pending dependent claims are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Rejection(s) under 35 U.S.C. § 103

Claims 7-10, 17, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buhan in view of US Pub. No. 2001/0002486 ("Kocher"). To the extent that this rejection may still apply, this rejection is respectfully traversed.

As described above Buhan fails to disclose or render obvious the limitations of the amended independent claims. Further, Kocher fails to supply that which Buhan lacks. Specifically, Kocher discloses an RSA encryption/decryption algorithm. However, Kocher fails to disclose or render obvious combining two keys to obtain a pairing key which is used to decrypt common data across a plurality of receiving decoding system pairs, as required by (ii) above. Accordingly, independent claims 1 and 15 are patentable over Buhan and Kocher, considered alone or in combination. Dependent claims 7-10 and 17-18 are patentable for at least the same reasons. Withdrawal of this rejection is respectfully requested.
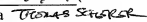
Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number

listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591

(Reference Number 17250/017001).

Dated: August 3, 2010   Respectfully submitted,

By _____ # 45,079

Jonathan P. Osha Thomas Stoerer
Registration No.: 33,986
OSHA · LIANG LLP
909 Fannin Street, Suite 3500
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant